LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-TR-674556

IAEA TECDOE 055 Outline

D. Shull

July 14, 2015

Disclaimer

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

IAEA TECDOC-055 – IAEA Handbook for Designing and Implementing Physical Protection Systems for Nuclear Material and Nuclear Facilities
(Revision of IAEA-TECDOC-1276)

Developed by Doug Shull
Gregg Protection Services under LLNL Contract
July 9, 2015

Background
Revision 5 of INFCIRC/225 was published as Nuclear Security Series No. 13(NSS No.13): Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities in 2011, and included a number of new or expanded concepts. The draft Implementing Guide for NSS No.13 (i.e., NST023, currently in development) incorporates and updates the contents of TECDOC-967. TECDOC-1276 was also taken into account in drafting Implementing Guide NST023, specifically in Chapter 4 on developing, implementing and maintaining an integrated physical protection system for nuclear facilities; however, TECDOC-1276 provides very detailed guidance for facility operators on the design, operation and maintenance of physical protection systems. Therefore, the drafters of NST023 recommended that TECDOC-1276 be revised. Because it was considered to contain potentially sensitive information, TECDOC-1276 was never publicly available, but copies were provided to Member States on request. In addition, at the time TECDOC-1276 was issued, there was no Nuclear Security Series. This NST055 document is planned as an NSS Technical Guidance that will be publicly available.

This outline is to be shared and discussed with the IAEA Technical Lead as the first input to the development of IAEA TECDOC-055 (NST055).

Tentative Outline Content of the proposed NST055 Technical Guidance

1. Introduction

NEEDS TO BE DEVELOPED

1.1 Background

Revise from *IAEA-TECDOC-1276 – 1.1*

1.2 Purpose

Revise from *IAEA-TECDOC-1276 – 1.2*

1.3 Scope

Revise from *IAEA-TECDOC-1276 – 1.3*

1.4 Structure

NEEDS TO BE DEVELOPED

2. Process of PPS Design and Analysis

IAEA-TECDOC-1276

Chapter 2: Process of Physical Protection System Design and Analysis

14.3. The Process of PPS Design

NST023 - 4.3 - PROCESS FOR DEVELOPING AND IMPLEMENTING A PPS - Not clear what is needed in 1276 that is not in IG?

NST023 Draft

Section 4

Process for developing and implementing a PPS

Approach for developing the PPS

Defence in depth

2.1 Prerequisites

NEEDS TO BE DEVELOPED

NST023 – 2.X – Quality Assurance

2.2 Define System Objectives

IAEA-TECDOC-1276

2.2. Define System Objectives

NST023 - 4.4. IDENTIFYING THE REQUIREMENTS FOR A PPS

NST023 Draft

Section 3

Graded approach

Identifying the requirements for a PPS (Phase 1)

2.3 Design the System

WILL INCLUDE INPUT FROM ITC

IAEA-TECDOC-1276

2.3. Design the System

5.9. System Design Criteria

NSS 10

3. DESIGN BASIS THREAT

NST023 - 4.5.1. Design phase

NST023 Draft

Section 4

Design phase (Phase 2)

2.4 Evaluate the System Design

IAEA-TECDOC-1276

1.5. Performance-Based Design and Evaluation

2.4. Evaluate the System Design

NST023 - 4.5.2. Evaluation phase

NST023 Draft

Section 4

Design and evaluation of the PPS

2.5 Re-design process

IAEA-TECDOC-1276

2.5. Redesign Process

NST023 Draft

Section 3

Risk-based physical protection systems

3. Physical Protection System

WILL INCLUDE INPUT FROM ITC

IAEA-TECDOC-1276

Chapter 5: Physical Protection Systems

14.2. Physical Protection Systems

3.1 Key Functions of the PPS

WILL INCLUDE INPUT FROM ITC

IAEA-TECDOC-1276

5.1. Objective of a Physical Protection System

5.3. Physical Protection System Functions

5.4. Deterrence

5.5. Detection – Discovering Adversary Action

5.6. Delay

5.7. Response – Defeating an Adversary

5.8. Characteristics of a Physical Protection System

5.11. Summary

NST023 - 4.6. KEY FUNCTIONS OF A PHYSICAL PROTECTION SYSTEM

3.2 System Integration

Security by Design

Integrating physical protection principles as early as possible in the facility's lifetime is commonly referred to as security by design.

The intent of security by design is to design a new nuclear facility so that the required level of security is provided in a cost-effective way that is compatible with operations, safety and NMAC. Security by design is best implemented through a structured approach in which a State's nuclear security objectives are considered and fully taken into account in design decisions for the entire lifetime of the facility, starting with planning of the facility, and through the design, construction, operational and decommissioning phases. (NST023, 4.9)

Integrated physical protection system

An effective nuclear security program is based on an integrated physical protection system that takes into account physical protection, nuclear material accounting and control (NMAC), information protection, and computer security that has seamless integration with facility operational systems such as engineered safety and operational systems, radiation protection, emergency preparedness measures, and emergency response.

Along with detection, delay, response mentioned above, measures also include mitigation capacities of safety, radiation protection and NMAC provisions. Their synergetic effect should be established and formally integrated within the comprehensive protection approach. (NSS 8 – 5.2).

When physical protection systems are evaluated in conjunction with other systems such as engineering safety aspects, an integrated team may be formed, including physical protection experts.

PP Systems

A physical protection system integrates the PPS components of people, procedures, and equipment for the protection of assets or facilities from unauthorized removal of nuclear material and /or sabotage. The PPS functions of detection, delay, and response are accomplished through PPS sub-systems of access control, barriers, intrusion detection, CCTV assessment, communication, material accounting and control, and facility operational systems.

The Access Control System (ACS) controls the movement of authorized personnel and detects and denies the unauthorized movement of personnel. The Intrusion Detection System (IDS) monitors potential facility path elements through sensors to identify that someone or something is moving through these facility path elements unauthorized. The CCTV surveillance/assessment system provides the protective force with the capability of surveillance, assessing, and identifying whether this intrusion is an adversary or friendly act. These sub-systems communicate electronically with each other to insure a timely detection and assessment of whether this is an adversary act or not. The electronic communication goes to the Central Alarm Station for initiation of a timely security response by the operator should one be necessary. The different components of these subsystems are covered in detail in Section 4 of this document.

Nuclear Material Accounting and Control

NMAC provisions are designed to keep a strict inventory of all nuclear material and to register an alarm if the material balance shows a discrepancy. MC&A also enables the operators to: (a) know precisely the quantity and type of all inputs and outputs of nuclear material in their facilities; (b) always be aware of the location, use, movement and transformation of nuclear material; and (c) detect any anomalies concerning the management of nuclear material.

Implementing preventive and protective measures to counter the insider threat is usually much more difficult than implementing measures to counter the outsider threat, due to the access, knowledge, authority and attributes of insiders. Thus, although already partially addressed for the outsider threat, any elements that could provide protection against the insider threat should be considered. (NSS 8 – 5.2)

Engineered Safety and Operational Systems

For nuclear safety purposes, design criteria such as redundancy or diversity in systems and equipment that are important to safety, or layout criteria such as physical or geographical separation or segregation of these systems or equipment, are introduced at the design phase of the facility or transport package. These provisions can improve protection against sabotage by requiring more preparation, more equipment and more time for an insider to commit a malicious act. Consequently, they could be of significant efficiency to deter, prevent or delay acts of sabotage by insiders or to mitigate or minimize the radiological consequences. (NSS 8 – 5.2)

Other examples of diverse systems may be the use of continuous air monitors (CAMs) or glove box negative pressure alarms to both provide protection for operator personnel and to provide alarms for potential malevolent acts of sabotage or theft. These systems could be integrated into the operator protection strategies by either established procedural or automated alarm communications between safety and security organizations for certain operational or event conditions.

Radiation protection measures, such as the limitation of access to specific areas and radiation protection devices, could contribute to both deterring and preventing unauthorized removal or sabotage by insiders. Radiation protection measures such as thick concrete walls or shielding barriers can provide both safety measures for personnel and increase adversary delay time to target locations.

Information Protection

Confidentiality (security of information). Information on security measures or sensitive targets (e.g. the location of the nuclear material inventory, site maps or specific drawings of equipment, systems or devices that represent the design features of specific targets, lock combinations, passwords and mechanical key designs) could help insiders successfully to perform a malicious act. This information should be kept confidential so that only those who need to know are permitted access to it. In addition, information addressing potential vulnerabilities in physical protection systems should be highly protected and compartmentalized, as it could facilitate the unauthorized removal of nuclear material or an act of sabotage. Compartmentalization means dividing information into separately controlled parts to prevent insiders from collecting all the information necessary to attempt a malicious act. Special attention should be paid to electronic information. Ensuring confidentiality will mean that insiders would have to make additional

efforts to carry out unauthorized removal of nuclear material or an act of sabotage, during which they could be deterred or detected. (NSS08, 5.3 (c))

Computer Security

All disciplines of security interact and complement each other to establish a facility's security posture as may be defined in the SSP (see Fig. 1). A failure in any of the disciplines of security could impact the other domains and cause extra requirements on the remaining aspects of security. Computer security is a cross-cutting discipline that has interactions with all other areas of security in a nuclear facility. (NSS 17 - 2.3)

NST023 – Safety Security Interface

4. Physical Protection System Measures

NST023 4.9. PHYSICAL PROTECTION MEASURES

4.9.1. Protection areas and layers

NST023 Draft

Section 4

Deterrence

Protection areas and layers

4.1 Intrusion Detection

WILL INCLUDE INPUT FROM ITC

NSS 7 - 2.4

4.2 Video Technology

WILL INCLUDE INPUT FROM ITC

IAEA-TECDOC-1276

7.3. Camera and Lens

7.4. Image Format

7.5. Lenses

7.6. Distance and Width Approximation

7.7. Maximum Usable Zone Length

7.8. Camera Mounting/Support Structures

4.3 Alarm Assessment

WILL INCLUDE INPUT FROM ITC

IAEA-TECDOC-1276

Chapter 7: Alarm Assessment

7.2. Video Alarm Assessment System

7.9. Lighting System

7.10. Video Transmission System

7.11. Video Switching Equipment

7.12. Video Recording

7.13. Video Monitors

7.14. Video Controller

7.15. Additional Design Considerations

7.16. Alarm Assessment by the Guard Force

4.4 Central Alarm Station

WILL INCLUDE INPUT FROM ITC

IAEA-TECDOC-1276

Chapter 8: Alarm Communication and Display

8.2. Evolution of Alarm Reporting System

8.3. Alarm Communication Systems

8.4. Alarm Display

8.5. Audible Devices

8.6. Alarm Assessment.

8.7. Operator Controls

8.8. Equipment Placement

8.9. Other Considerations

8.11. Evolution of Alarm Reporting System

NST023 - 4.9.2. Central alarm station

4.5 Access Control Systems

WILL INCLUDE INPUT FROM ITC

IAEA-TECDOC-1276

Chapter 9: Access Control Systems

9.2. Control of Personnel Access

9.3. Personal Identity Verification

9.4. Personnel Tracking

9.7. Locks

9.8. Seals

NST023 - 4.9.4. Access control systems

4.6 Search Systems

WILL INCLUDE INPUT FROM ITC

IAEA-TECDOC-1276

9.5. Contraband Detection

9.6. Nuclear Material Detectors

4.7 Barriers

WILL INCLUDE INPUT FROM ITC

IAEA-TECDOC-1276

Chapter 10: Delay – Barriers

10.2. Role of Barriers

10.3. Types of Barriers

10.4. Barrier Philosophy

10.5. System Considerations

10.6. Aspects of Penetration

10.8. Perimeter Barriers

10.9. Fences

10.10. Gates

10.11. Vehicle Barriers

10.12. Structural Barriers

10.13. Walls

10.14. Doors.

10.15. Windows

10.16. Utility Ports

10.17. Roofs and Floors

10.18. Dispensable Barriers

10.19. Testing Barriers

NST023 - 4.9.3. Physical barriers

4.9.6. Protection measures for stand-off sabotage attacks

4.8 Response

WILL INCLUDE INPUT FROM ITC

IAEA-TECDOC-1276

Chapter 11: Response and Communication

11.2. Role of Response Forces

11.3. Interruption and Communications

11.4. Deployment of the On-Site and Off-Site Response Force

11.5. Neutralization

NST023 - 4.9.5. Guards and response forces

What about adding Guards to this section?

4.9 Network design, Power supply and other support systems

Other Support Systems material may need to be developed

NSS-17

Computer Security at Nuclear Facilities (for Network Design)

8.10. Other Considerations = Emergency Power, Backup Considerations

4.10 New/emerging technologies for PPS

NEEDS TO BE DEVELOPED

NSS 13 Section 3.2

NSS023 - 4.9.7. Protection measures for airborne and waterborne attacks

5. Evaluation of PPS Effectiveness

Refer to NUSAM Methodology plus a summary section

IAEA-TECDOC-1276

Chapter 12: Analysis and Evaluation Techniques

NST023 – 4.5.2.1. Physical protection evaluation and performance testing by the operator

5.1 Overview of evaluation process

Refer to NUSAM Methodology plus a summary section

IAEA-TECDOC-1276

12.2. Adversary Paths

12.3. Effective Measures

5.2 Performance testing of technical measures (individual components system elements)

IAEA-TECDOC-1276

2.4 Evaluate the System Design = Testing the System, Methods to Evaluate a PPS

Refer to NUSAM Methodology

NST023 – 3.3.2 System evaluation, including performance testing: requirements by the State

5.3 Evaluation of personnel, plans and procedures, including protection against insiders

IAEA-TECDOC-1276

3.5. Insider Threats

5.10. Operational Considerations

5.2. Physical Protection Plan

NSS 8

5.2, DEVELOPMENT OF A COMPREHENSIVE APPROACH

6. EVALUATION OF PREVENTIVE AND PROTECTIVE MEASURES

6.1. OBJECTIVES AND OVERVIEW OF THE EVALUATION PROCESS

6.2. EVALUATION OF PREVENTIVE MEASURES

6.3. EVALUATION OF PROTECTIVE MEASURES

NST041- draft

5.0 EVALUATION OF MEASURES

NST023 – 3.5 IDENTIFICATION AND ASSESSMENT OF THREATS

Insiders and NMAC computer security

4.5.2.3. Additional evaluation considerations for insider threats

5.4 Overall System Evaluation

Refer to NUSAM Methodology

IAEA-TECDOC-1276

12.4. Computer Modeling Analysis

12.5. Empirical Methods

6. Facility Integrated Nuclear Security Management

Management Responsibility

Site security is primarily a management responsibility, specifically of senior management, to ensure that legislative and regulatory requirements are fully met through the implementation of the site security plan (SSP). All disciplines of security (including personnel, physical,

information and computer) interact and complement each other to establish a facility's security posture as may be defined in the SSP. A failure in any of the disciplines of security could impact the other domains and cause extra requirements on the remaining aspects of security. Computer security is a cross-cutting discipline that has interactions with all other areas of security in a nuclear facility. (NSS 17 - 2.3)

Safety and Security

Many diverse organizations are concerned with nuclear security. These include, in particular, individuals, organizations and institutions engaged in protecting radioactive material and their associated locations, facilities and transport; some of these bodies may have little technical knowledge about nuclear or other radioactive material. This lends greater weight to the need for effective structural, communication, information and exchange systems, and the integration of the functions of these diverse organizations into a unified nuclear security culture. Safety and security cultures coexist and need to reinforce each other because they share the common objective of limiting risk. There will be occasions where there are differences between safety and security requirements. Therefore, an organization in charge of nuclear matters has to foster an approach that integrates safety and security in a mutually supporting manner. (NSS 7 - 2.4)

The operator has the primary responsibility for the safety and physical protection of the nuclear facility. It is suggested that operators adopt, through their integrated management system, an integrated and coordinated approach to developing and implementing proposed changes in order to avoid unintended degradation of safety and physical protection or of emergency preparedness arrangements. (NST23 - 4.148)

Integration of physical protection

The highest levels of the operator's management need to be aware of and endorse the integration of physical protection measures into facility operations. It is equally important that management encourages a strong nuclear security culture as described in [13] and discussed briefly in Section 3.7.1. (NST023 - 4.11)

For an integrated approach to implementation of physical protection, the operator of a nuclear facility identifies all potential targets for unauthorized removal and sabotage and implements all the required protection measures in a graded manner based on the State's regulatory approach. Depending on the type of nuclear facility, either the sabotage or the unauthorized removal targets may require a higher level of protection, but in all cases the appropriate levels of protection should be implemented for all targets. This is what is intended by the recommendation to apply the "more stringent applicable requirements" in (NST023 - 4.12)

7. Security of Nuclear Material in Transport

IAEA-TECDOC-1276

Chapter 13: Transportation

13.2. Transportation – Assumptions

13.3. Detection Requirements

13.4. Delay Requirements

13.5. Response Requirements

13.6. Sabotage

13.7. Measures for Lower Categories of Nuclear Material

14.4. Transportation

NST023 – 3.3.1.1. Performance-based method

4.9.8. Transport of nuclear material

NSS 9 - Security in the Transport of Radioactive Material

Section 2 DESIGN AND EVALUATION OF SECURITY MEASURES

NST17

New Topics: Conveyance, Communications, Transportation Control Center

Issues: What about varying routes, etc., transfer points; stopping along the way?

8. Physical Protection aspects addressed in detail in other existing or planned NSS documents

NEEDS TO BE DEVELOPED

Sections from Current TECDOC not currently identified in the Revised Version

1.6. The Physical Protection Plan

1.7. Determination of Trustworthiness

1.8. Emergency Plans

1.9. Education and Training

Chapter 3: Threat Definition

3.2. Define the Threat

3.3. Threats Define Requirements

3.4. Tactics and Actions of Adversaries

3.5. Insider Threats

3.6. Motivations of the Adversary

3.7. Adversary Capabilities

3.8. Gathering Threat Information

3.9. Organize Threat Information

Chapter 4: Target Identification

4.1. Target Identification

4.2. Consider the Undesirable Consequences

4.3. Targets

4.4. Techniques for Target Identification

4.5. Logic Diagrams (Fault Trees)

NST023 Sections Not Included so far

4.10 – NMAC

4.11 – Security of Sensitive Information

4.12 – Protection of Computer Based Systems

Other Comments

What about QA and Sustainment?

What about standoff?

What about security/contingency plans?

What about security by design?

What about Security Organization?

Remark: section at end of 4.1 ties into security during the lifecycle of a facility

Remark: Table 3 maps NSS 13 requirements to PP measures (pg 59 in word doc)

Remark: Appendix III maps Recommendations in NSS 13 to sections of NST 23